

MEMORANDUM FOR:

Jim McDonald wants a call re ISOO initiatives. I have attached a copy of the memo sent by you to DDA on the 25th of March and a copy of a memo from to the DDA which references OS's memo.



Done

OS Registry

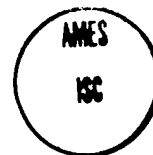


Date 4/9/86

TRANSMITTAL SLIP		DATE
TO:		<i>2 April</i>
ROOM NO.		<i>Director of Security</i>
BUILDING		
<div></div>		
<i>EO <u>rym</u></i>		
<i>D/S _____</i>		
<i>C/Policy/PPS _____</i>		
FROM:		
ROOM NO.	BUILDING	EXTENSION

STAT

LOGGED

OIS*125*86
4 APR 1986

MEMORANDUM FOR: Deputy Director for Administration

FROM:



Director of Information Services

STAT

SUBJECT: Information Security Oversight Office
Initiatives presented to the National
Security CouncilREFERENCE: Attached Office of Security memorandum for
DDA signature to the DCI

1. This memorandum provides additional information for your consideration regarding four of the information security initiatives forwarded to the National Security Council (NSC) on 14 November 1985 by the Director, Information Security Oversight Office (ISOO).

2. Background: The Director of ISOO chaired an interagency committee to study ways of improving the Government-wide information security system. This Agency, as well as the rest of the Intelligence Community, was represented on the committee. Each agency studied a particular aspect of the information security system and proposed measures they believed would improve the system. ISOO reviewed all of the proposals, discarded some, re-scoped others and finally selected thirteen to go forward to the National Security Council as ISOO initiatives. When forwarding the initiatives to the NSC, D/ISOO neglected to point out the disagreement among the participating agencies concerning the merit of some of these initiatives. Although the D/ISOO is aware of the Agency opposition to a number of these initiatives, he did not see fit to make it a part of his official correspondence to the NSC. These initiatives have also gained additional support from the Senate Select Committee on Intelligence (SSCI) and the Stillwell Working Group. The Agency specifically opposed the following four initiatives:

Initiative No. 1 - That ISOO issue a directive on security education that includes the establishment of minimum requirements for mandatory training of classifiers of original and derivative classification decisions and the use of classification guides.

OS REGISTRY

Initiative No. 2 - That ISOO issue a directive on agency self-inspections that establishes minimum criteria for internal oversight, including a requirement that each agency routinely sample its classified product.

Initiative No. 3 - That the President amend E.O. 12356 and ISOO amend Directive No. 1 to (i) require employees to report instances of improper classification and (ii) require that agencies provide an effective means for employees to challenge classification decisions free from the fear of retaliation.

Initiative No. 13 - That the President call upon the Attorney General to revise existing guidelines on investigations of unauthorized disclosures.

3. In the attached referent memorandum, the Office of Security (OS) cautions against an erosion of DCI special authorities only in Initiatives 1 and 13. I believe the same potential for erosion exists in ISOO Initiative No. 2. Although internal oversight to ensure against unnecessary or improper classification (Initiative No. 2) would be less difficult for the Agency to deal with than mandatory training of our classifiers (Initiative No. 1), it is, nonetheless, an encroachment on the DCI's special authorities. This initiative, if adopted, would permit ISOO to set internal Agency standards and procedures for inspections. If you choose to recommend DCI action to preserve his special authorities on these issues, I suggest that ISOO Initiative No. 2 be included with Initiatives Nos. 1 and 13.

4. Further, I recommend that this Agency continue to oppose ISOO's Initiative No. 3 in its entirety. There are two issues involved in Initiative No. 3: one, the "requirement" that all federal employees challenge classification decisions they believe to be improper; and two, that agencies provide an "effective means" for employees to challenge classification decisions free from the "fear of retaliation." OS recommends continued opposition to the "requirement" to challenge classification decisions but accepts the statement that there is a need to provide "effective means" for employees to challenge classification decisions. I disagree. This Agency already has an effective means for employees to challenge or question classification decisions. An employee wishing to question or challenge the classification or classification level of a document, can contact the the Agency Security Classification Officer (ASCO) and discuss these concerns. Although classification challenges in this Agency are rare, classification questions are fairly frequent and are routinely referred to the ASCO. If the ASCO is unable to resolve the question or problem, an employee has recourse to the Director, ISOO. Pursuant to E.O. 12356, Sec 5.2, (b) (6) the Director, ISOO shall consider and take action on complaints and suggestions with respect to the administration of the information security program. This

procedure has been used successfully in the past by individuals questioning the classification of documents. Other than using the phrase "fear of retaliation," as part of the initiative, ISOO has not offered, nor am I aware of, evidence of any retaliation against government employees or other individuals who have questioned classification decisions. Finally, we do not oppose the right of an employee to challenge or question a classification decision. Our opposition is based instead on concern over the administrative burden that would be placed on the Agency with no additional advantage to the Agency or the individual.

5. Although we have discussed our concerns with both the Office of Security and the Office of General Counsel, we have been unable to persuade either to our point of view. Nevertheless, I feel obliged to bring these issues to your attention. If you agree with our comments, we are prepared to revise the OS memorandum to the DCI to incorporate OIS concerns.



STAT

Attachment

DDA/OIS/IRMD/IME dbm (31 March 86)

STAT

Distribution:

Original & 1 - Addressee w/atts
1 - DDA Subject
✓1 - D/Security
1 - C/Policy Branch/OS
1 - OIS subject
1 - OIS chrono
1 - IRMD chrono
1 - IMB/IRMD Subject BLIA-2
1 - IMB/IRMD Chrono
1 - EME/IMB

ADMINISTRATIVE - INTERNAL USE ONLY

ROUTING AND RECORD SHEET

SUBJECT: (Optional) Information Security Initiatives Presented to the National Security Council by the Director, Information Security Oversight Office				
FROM: [Redacted] Director of Security		EXTENSION		NO.
				DATE 25 MAR 1986
TO: (Officer designation, room number, and building)		DATE		OFFICER'S INITIALS
		RECEIVED	FORWARDED	
1.	D/OIS 1205 Ames			<p>Attached for your signature is a proposed alert to the DCI regarding certain ISOO initiatives that enjoy the support of the NSC staff and have been embraced by the SSCI in its draft report currently under review by the SIG-I.</p> <div style="border: 1px solid black; height: 150px; width: 250px; margin: 10px auto;"></div>
2.				
3.	DDA 7D17 HQS			
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

STAT

STAT

STAT

ADMINISTRATIVE - INTERNAL USE ONLY

MEMORANDUM FOR: Director of Central Intelligence

FROM: Richard J. Kerr
Deputy Director for Administration

SUBJECT: Information Security Initiatives Presented to
the National Security Council by the Director,
Information Security Oversight Office (U)

This memorandum contains information pertinent to an item we understand will be considered by the National Security Council. Aspects of this have potential to erode your authority to protect intelligence sources and methods information and require that you take action at the NSC level if you wish to prevent this erosion. (U)

1. Background: The Director of the Information Security Oversight Office (ISOO) has forwarded 13 initiatives for consideration by the National Security Council. In presenting his initiatives, D/ISOO failed to document the strong objections that CIA raised concerning a number of them. These initiatives have been favorably reviewed by the Senate Select Committee on Intelligence (SSCI) and, if endorsed by the NSC, they will be given further support in General Stilwell's draft report soon to be forwarded for your review and endorsement. (A/IUO)

2. Two of the initiatives are in conflict with your statutory authority to protect sources and methods: (A/IUO)

ISOO Initiative #1 regarding Overclassification/Unnecessary Classification - That ISOO issue a directive on security education that includes the establishment of minimum requirements for mandatory training of classifiers of original and derivative classification decisions and the use of classification guides.

CIA Position: This initiative would permit ISOO to, in effect, mandate the qualifications which all Government employees must meet before being authorized to classify information. This initiative would give ISOO control over who in CIA is permitted to make classification decisions. It is our view that the authority should remain with the

OS 5 2070

ADMINISTRATIVE - INTERNAL USE ONLY

ADMINISTRATIVE - INTERNAL USE ONLY

DCI to decide who should or should not be permitted to make CIA classification decisions. We would have no objection if ISOO were to develop voluntary qualifications guidelines for classifiers as opposed to mandatory requirements. (A/IUO)

ISOO Initiative #13 regarding Unauthorized Disclosures - That the President call upon the Attorney General to revise existing guidelines on investigations of unauthorized disclosures. (U)

CIA Position: The initiative, as written, fails to take into account the fact that national security equities are what should drive the development of guidelines for Intelligence Community investigations in this area. The initiative does not recognize the distinction between investigations by the Community for the purposes of identifying those who make disclosures, of preventing future disclosures, and of determining the extent of damage done, as opposed to investigations by the FBI for purposes of criminal prosecution. Although the Community must vigorously support criminal prosecutions of unauthorized disclosures in those cases where prosecutions would not compromise the national security, the investigations done by the Community are not done for the purpose of gathering evidence for such prosecutions; the independent character of Intelligence Community investigations must be preserved. Nonetheless, we do find it commendable that D/ISOO is willing to join the fight against unauthorized disclosures. (A/IUO)

3. Another of the initiatives, while not a direct erosion of DCI authority, is logically flawed and has the potential to create an administrative nightmare. (U)

ISOO Initiative #3 regarding unnecessary classification - (i) That employees be required to report all instances of improper classification (overclassification, underclassification, unnecessary classification or procedurally incorrect classification); and (ii) that agencies provide an effective means for employees to challenge classification decisions free from the fear of retaliation. (U)

CIA Position: The original objective pertaining to this recommendation is to encourage persons who believe information is improperly classified to bring this to the attention of responsible officials. We believe part (ii) of the initiative is responsive to this goal. However, part (i) requires all federal workers to report, in effect,

ADMINISTRATIVE - INTERNAL USE ONLY

ADMINISTRATIVE - INTERNAL USE ONLY

their opinions about classification decisions with which they may disagree. It is patently unfair to hold employees at risk of censure for failing to report an opinion, particularly when the receiving employee's opinion would be, in most cases, less informed than that of the originator. Moreover, since virtually any classification discrepancy, no matter how minor, would be required to be reported, this initiative could well create an administrative burden of monstrous proportions. In sum, part (ii) seems to provide a remedy for any serious breach of classification rules. Part (i) should not be implemented; existing ISOO inspection procedures and others currently being recommended are the proper remedies for minor or technical irregularities. (A/IUO)

4. Recommendation: It is recommended that you raise the above considerations when the ISOO initiatives are discussed by the National Security Council. (A/IUO)

Richard J. Kerr

:OS/EO/PPS, (24 Mar 86)!

STAT

!Distribution:!
! Orig - Adse!
! 1 - ER!
! 1 - D/OIS!
! 2 - DDA!
! ① - D/S!
! 1 - OS Registry!
! 1 - PPG Chrono!
! 1 - Policy Br.!

ADMINISTRATIVE - INTERNAL USE ONLY